UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

UNITED STATES OF AMERICA	)	
	)	
v.	)	NO. 3:10-00009
	)	
JEREMY SETH TUMMINS	)	

MEMORANDUM AND ORDER

Defendant Tummins, through counsel, has filed his Motion To Compel Discovery pursuant to Rule 16 of the Federal Rules of Criminal Procedure and the due process clauses of the Fifth and Fourteenth Amendments to the Constitution of the United States (Docket Entry No. 27). By this motion defendant seeks an order compelling the Government to produce for inspection and copying seven enumerated items. The Government has filed a response in opposition (Docket Entry No. 31), and defendant Tummins has filed a reply (Docket Entry No. 35).

This motion to compel and defendant Tummins's motion for oral argument (Docket Entry No. 29) were referred to the undersigned Magistrate Judge for a hearing and for disposition (Docket Entry No. 30).

The Court granted defendant Tummins's related motion for oral argument (Docket Entry No. 32) and conducted a hearing on February 16, 2011. Following this hearing, the Court permitted both the Government and the defendant to submit in writing any further authority or arguments that they wished.

For the reasons stated below, the Court **GRANTS** in part and **DENIES** in part defendant Tummins's motion to compel.

Statement of the Case

Defendant Tummins was indicted on January 13, 2010, and charged with the offenses of receipt and possession of child pornography in violation of Title 18, United States Code, Sections 2252A(a)(2)(A), 2252A(b), and 2252A(a)(5)(B) (Docket Entry No. 1). These charges resulted from a search warrant executed by the Dickson County Sheriff's Office on or about May 18, 2009, during which two computers allegedly containing images of child pornography were seized from defendant's home.

Following a series of telephone conferences and an exchange of correspondence between counsel (Docket Entry Nos. 31-1 through 31-4), defendant Tummins filed the subject motion to compel discovery. By his motion, defendant seeks an order requiring the Government to produce for inspection and copying the following enumerated items:

1. An index of all the files on both computers including all their metadata (.csv format);

2. An index of all files determined to be child pornography including all the metadata for each file as well as how it was determined to be child pornography;

3. Complete and up to date logs, including any logs or records created during the initial online portion of Levasseur's

[Detective Scott Levasseur, the Government's forensic computer expert] investigation; logs to all activity conducted within the Forensic Tool Kit (FTK) software along with any other software used during the examination of the computers up to this point (.txt or .csv format);

4. A list of ALL software used during the initial online investigation and during the entire examination of both the computers. The list should include name, version information, manufacturer and licensing information for each product (.txt, .pdf or .doc format);

5. Fully functional copies of the same versions of GnuWatch and Peer Spectre software that were used by Det. Levasseur for independent testing and verification;

6. A copy of the SHA1 database of known child pornography images that was used during this investigation; as well as information of where the database was obtained, who maintains it, how often it's updated, who and how it's distributed, the criteria used to conclude and/or add files of "known child pornography" to the database and how files are removed from the database if they are found not to be actual child pornography;

7. A copy of the hard drive with the alleged child pornography redacted.

The Court will address each item of discovery sought in the order presented in defendant's motion.

Discussion

1. An index of all the files on both computers including all their metadata. With respect to this request, the Government in its response has stated that to the extent it possessed such an index, it was included in Detective Levasseur's forensic report and has been disclosed to the defendant. The Government takes the position that there is no basis for any further disclosure because Rule 16 does not require the Government to create and produce an index that is not in its possession (Docket Entry No. 31 at 8). Nevertheless, in what the Government describes as an effort to compromise, the Government has agreed to create an index of all files on both computers, including metadata, and to provide that index to defendant (Id.). In view of the Government's willingness to produce this material voluntarily, the Court **GRANTS** defendant's motion with respect to the requested index.

2. An index of all files determined to be child pornography including all the metadata "as well as how it was determined to be child pornography." With respect to this request, the Government states that to the extent it possessed such an index, the index was included in Detective Levasseur's forensic report or was recreated by the Government in response to a request received from the defendant for a list of images that the Government claims were child pornography, and that both of these lists have been disclosed to the defendant. Although the

Government insists that Rule 16 does not require the Government to create and produce any additional index, it nevertheless has created an index of suspected child pornography files, including metadata, and has agreed to provide this index to the defendant. Given the Government's willingness to provide this index of alleged child pornography voluntarily, the Court **GRANTS** defendant's motion to compel discovery of such an index. With respect to the remainder of this request, including the inquiry of "how it was determined to be child pornography," the undersigned Magistrate Judge finds that this request exceeds the requirements of Rule 16(a)(1)(E), and that this portion of the request, therefore, must be **DENIED**.

3. Complete and up to date logs, including any logs or records created during the initial online portion of Levasseur's investigation; logs to all activity conducted within the Forensic Tool Kit (FTK) software along with any other software used during the examination of the computers up to this point. Defendant asserts in his memorandum (Docket Entry No. 28 at 5) that he is entitled to this discovery pursuant to Rule 16 of the Federal Rules of Criminal Procedure. In response, the Government insists that while such logs are in the Government's possession, the defendant has made no showing that these logs are discoverable under any of the three subparagraphs of Rule 16(a)(1)(E). Moreover, the Government maintains that the demanded logs are work product

protected from discovery pursuant to Rule 16(a)(2). The undersigned Magistrate Judge finds that, beyond a general citation to Rule 16, defendant has made no showing that the requested logs are discoverable under any of the subsections of Rule 16(a)(1)(E), and, therefore, defendant's motion to compel production of the described logs must be **DENIED**.

4. A list of ALL software used during the initial online investigation and during the entire examination of both the computers, including name, version information, manufacturer and licensing information for each product. Again, defendant makes the general argument that he is entitled to discovery of this information pursuant to Rule 16. In response, the Government maintains that, to the extent it is in possession of such a list, the list is included in Detective Levasseur's search warrant affidavit and forensic report, both of which have previously been disclosed to defendant. The Government argues that Rule 16 does not require it to create and produce a further list not currently in its possession. In addition, the Government further argues that defendant has made no showing that such a list is discoverable pursuant to the three subsections of Rule 16(a)(1)(E). From a review of the record, the undersigned Magistrate Judge finds that defendant has failed to make a showing that the Government is required to create and produce a list not already in its possession, or that such a list is otherwise discoverable pursuant

to the provisions of Rule 16. Therefore, defendant's motion to compel discovery of a list of all software used during the Government's investigation or examination of the subject computers must be **DENIED**.

5. Fully functional copies of the same versions of GnuWatch and Peer Spectre software that were used by Det. Levasseur for independent testing and verification.

6. A copy of the SHA1 database of known child pornography images that was used during this investigation, as well as information of where the database was obtained, who maintains it, how often it's updated, who and how it's distributed, the criteria used to conclude and/or add files of "known child pornography" to the database and how files are removed from the database if they are found not to be actual child pornography. Defendant argues generally that he is entitled to discovery of the described software and database pursuant to the provisions of Rule 16. In response, the Government insists that this material is not discoverable because there has been no showing that any of the three subsections of Rule 16(a)(1)(E) apply either to the requested software or to the requested database. Moreover, the Government asserts that it cannot provide fully functional versions of the requested software because these programs connect to law enforcement databases containing nonpublic information, and, similarly, that the SHA1 database is a law enforcement database.

From a review of the record, the undersigned Magistrate Judge finds that defendant has failed to make a showing that the requested software and database satisfy any of the three subsections of Rule 16(A)(1)(E), and, therefore, that defendant's motion to compel discovery of this material must be **DENIED**.

7. A copy of the hard drive with the alleged child pornography redacted. Defendant seeks an order requiring the Government to produce forensic copies of the hard drives of the two computers seized from defendant, from which all files alleged by the Government to contain child pornography have been electronically redacted. In response, the Government argues that production of the requested forensic copy of the hard drive to defendant is prohibited by 18 U.S.C. § 3509(m). This statute provides as follows:

> (1) In any criminal proceeding, any property or material that constitutes child pornography (as defined by section 2256 of this title) shall remain in the care, custody, and control of either the Government or the court.
>
> (2)(A) Notwithstanding Rule 16 of the Federal Rules of Criminal Procedure, a court shall deny, in any criminal proceeding, any request by the defendant to copy, photograph, duplicate, or otherwise reproduce any property or material that constitutes child pornography (as defined by section 2256 of this title), so long as the Government makes the property or material reasonably available to the defendant.
>
> (B) For the purposes of subparagraph (A), property or material shall be deemed to be reasonably available to the defendant if the Government provides ample opportunity for inspection, viewing,

> and examination at a Government facility of the property or material by the defendant, his or her attorney, and any individual the defendant may seek to qualify to furnish expert testimony at trial.

Although defendant's motion seeks a forensic copy of the computer hard drives from which all files containing child pornography have been redacted, the Government argues that it is technically impossible to be absolutely certain that all traces of child pornography have been removed from a forensic copy of these computer hard drives and, therefore, section 3509(m) prohibits production of redacted copies of the hard drives to defendant.

In addition, the Government argues that it has provided the defendant and his expert witness with "ample opportunity for inspection, viewing, and examination" of the subject computer hard drives at a Government facility, in compliance with 18 U.S.C. § 3509(m)(2)(B).

The undersigned Magistrate Judge conducted an evidentiary hearing on February 16, 2011. At that hearing defendant called as his sole witness James KempVanEe. KempVanEe is an employee of LogicForce Consulting, LLC, and serves as the company's Digital Forensic Lab Manager. Mr. KempVanEe has been employed by defendant as a computer forensic expert. The Government at the hearing conceded that Mr. KempVanEe is qualified by education, training and experience to testify as an expert on matters regarding computer forensic analysis.

Mr. KempVanEe testified that, using a forensic copy of the subject hard drives, a computer program known as EnCase could be used to overwrite the file contents of the 23 files[1] identified by the Government's computer forensic expert as containing child pornography while leaving the remainder of the file information intact. This process would replace the allegedly pornographic images in these 23 files with zeros such that the allegedly pornographic images would no longer exist on this forensic copy, but that all remaining computer data would remain intact for analysis by Mr. KempVanEe on behalf of the defendant. This would allow Mr. KempVanEe to determine such things as when and how the files allegedly containing child pornography were imported on this computer, the search terms that may have been used to locate and download these images, the dates on which these images were viewed and the time duration of any such viewings. According to Mr. KempVanEe, all such information would be material to a defense of this case.

On cross-examination by the Government, Mr. KempVanEe testified that the master file table would enable one to be sure that all files containing child pornography have been overwritten and redacted before providing a forensic copy of the subject hard

[1]At the hearing the parties expressed some uncertainty whether 23 or 28 computer files have been determined by the Government to contain child pornography. From correspondence of counsel contained in the record, it appears that the correct number is 23 files (Docket Entry No. 31-3).

drives to the defendant. Mr. KempVanEe conceded that it is "possible" that files containing fragments of images of children might reside in "unallocated space" of the hard drive if it existed there. However, according to Mr. KempVanEe, the Government's expert listed no file allegedly containing child pornography as having come out of unallocated space on these hard drives.

Mr. KempVanEe further testified that the restrictions imposed upon defense expert computer examiners by the Dickson County computer lab effectively prevented him from serving as a defense expert in this case. In particular, Mr. KempVanEe explained that, based upon the Government computer expert witness's report, the data to be examined on these two hard drives amounted to approximately 750 gigabytes of data. According to Mr. KempVanEe, the Government's expert witness required approximately 19 hours of computer time to create a file index of the hard drive of one computer and 7 hours to create a file index of the other. Access to these hard drives at the Dickson County computer lab is limited to Monday through Friday from 7:00 a.m. to 3:00 p.m. (Docket Entry No. 27-2).[2] The large amount of data to be examined, and the time required to complete such an examination, would require that the computer hardware and software owned by Mr. KempVanEe's employer remain unattended and inaccessible during

[2]As an alternative, the Government has offered to make these hard drives available at the Secret Service Field Office in Nashville. However, hours of access and other restrictions at this location would be similar to those in effect at the Dickson County computer lab.

nonbusiness hours in the offices of the Dickson County computer lab continuously for a period of several days. Mr. KempVanEe testified that this computer hardware and software costs his employer "thousands and thousands of dollars" and that his employer, LogicForce Consulting, LLC, would not permit its hardware and software to remain unattended overnight and on weekends in Government offices for the extended period required to complete a forensic analysis of these computer hard drives. Accordingly, the restrictions imposed by the Government effectively prevent Mr. KempVanEe and his employer from serving as a computer forensic expert witness on behalf of defendant in this case.

Secret Service Agent Lee Eaves was called as a witness by the Government. Mr. Eaves testified that he has worked as a computer forensic recovery specialist since 2005. Mr. Eaves testified that although he has worked on other cases involving charges of possession of child pornography, he has not worked on this case and is "very removed" and "very unfamiliar" with the facts of this particular case. Nevertheless, Mr. Eaves testified that, in his opinion, there is no way to ensure that no child pornography images remain after a digital redaction and that "a human error could be made." Mr. Eaves testified that, in his opinion, the only way to guarantee that no child pornography gets out is for the Government to maintain control of the hard drives. Although he admitted that he was not familiar with the thoroughness

of the forensic evaluation performed by the Government in this case, he questioned “what if we simply miss something?”

Rule 16(a)(1)(E)(iii) provides that the Government must permit the defendant to inspect and to copy data within the Government’s possession, custody or control if the data was obtained from or belongs to the defendant. Here, it is undisputed that the data on the two computer hard drives was obtained from defendant during the course of a search pursuant to a warrant.

The resolution of this motion raises at least two questions. First, what is the realistic possibility that recognizable child pornography will remain on this forensic copy of the hard drive despite digital redaction of the contents of all files identified by the Government as containing child pornography? Second, if there is a material possibility that child pornography will remain on the imaged hard drive despite redaction, has the Government provided an ample opportunity for inspection, viewing and examination of these hard drives at a Government facility, given the rules and restrictions that the Government seeks to impose?

The record in this case fails to answer the first question precisely. Mr. KempVanEe, on cross-examination by the Government, conceded that it is at least theoretically “possible” for fragments of files to be found in the unallocated space of the hard drive of a computer, “in the sense that anything is possible.”

However, Mr. KempVanEe minimized this possibility by testifying that, from Detective Levasseur's report, be searched the unallocated space on these hard drives for child pornography, and, according to his forensic report, he found no child pornography in the unallocated space. The Government's witness, Mr. Eaves, testified in substance that there is no way to ensure that no child pornography images remain in unallocated space on a hard drive and that the "possibility of trace images" would exist even after electronic redaction. Significantly, neither Mr. KempVanEe nor Mr. Eaves had examined the hard drives at issue in this case, and neither witness was able to quantify the likelihood that recognizable images of child pornography would remain on these drives following electronic redaction. From the testimony that was offered, however, the Court infers that the likelihood of child pornography remaining on a hard drive copy following redaction of the file contents of those files identified as containing child pornography would be relatively low.

Moreover, given the particular facts of this case, the undersigned Magistrate Judge finds that the restrictions imposed by the Government do not satisfy the requirements of section 3509(m)(2)(B) requiring the Government to provide "ample opportunity for inspection, viewing, and examination at a Government facility." Specifically, access to the subject hard drives in the Dickson County computer lab or the Secret Service

Field Office will be limited to 8 hours per day Mondays through Fridays. In addition, the rules provide that any electronic storage device brought into the Government facility must be erased, or "wiped," before it is permitted to be taken from the facility. The electronic data to be examined approximates 750 gigabytes, which required approximately 19 hours of continuous computer run time to index when examined by the Government expert. These facts, taken together, mean that a defense expert necessarily would be required to leave his hardware and software running unattended and inaccessible in Government offices, except during normal business hours, for the duration of an analysis that could take at least two weeks (Docket Entry No. 27-1 at 2). Mr. KempVanEe has clearly testified that his employer, which owns the hardware and software that Mr. KempVanEe proposes to use to conduct his forensic analysis of these hard drives, is unwilling to allow its equipment to remain inaccessible and unattended in a Government facility.

Following due consideration to the testimony of the parties and the record in this case, the undersigned Magistrate Judge finds that defendant's motion to compel the Government to produce a forensic copy of the two computer hard drives obtained from defendant from which all child pornography images have been redacted should be **GRANTED**. The Government shall electronically redact the file contents of all computer files identified by the Government as containing child pornography images and provide

forensic copies of such redacted hard drives to defendant within 14 days from entry of this order. These redacted hard drives shall be maintained in a secure location in the custody of defendant's forensic computer expert, and access to any data contained on these imaged hard drives shall be limited to the defense computer forensic expert and the defense attorney. These hard drives shall be used only for purposes of the present case, and no copy of any image of child pornography as defined by federal law shall be made. Upon completion of the hard drive examinations, these hard drives shall be returned to the Government. The defense forensic computer expert shall certify that, upon completion of the hard drive examinations, all files and any remnants or fragments of the hard drives have been permanently removed and deleted from any defense computer equipment.

It is so **ORDERED**.

s/ John S. Bryant
JOHN S. BRYANT
United States Magistrate Judge